Umbrella Enforcement API für kundenspezifische Integrationen

Inhalt

Einleitung

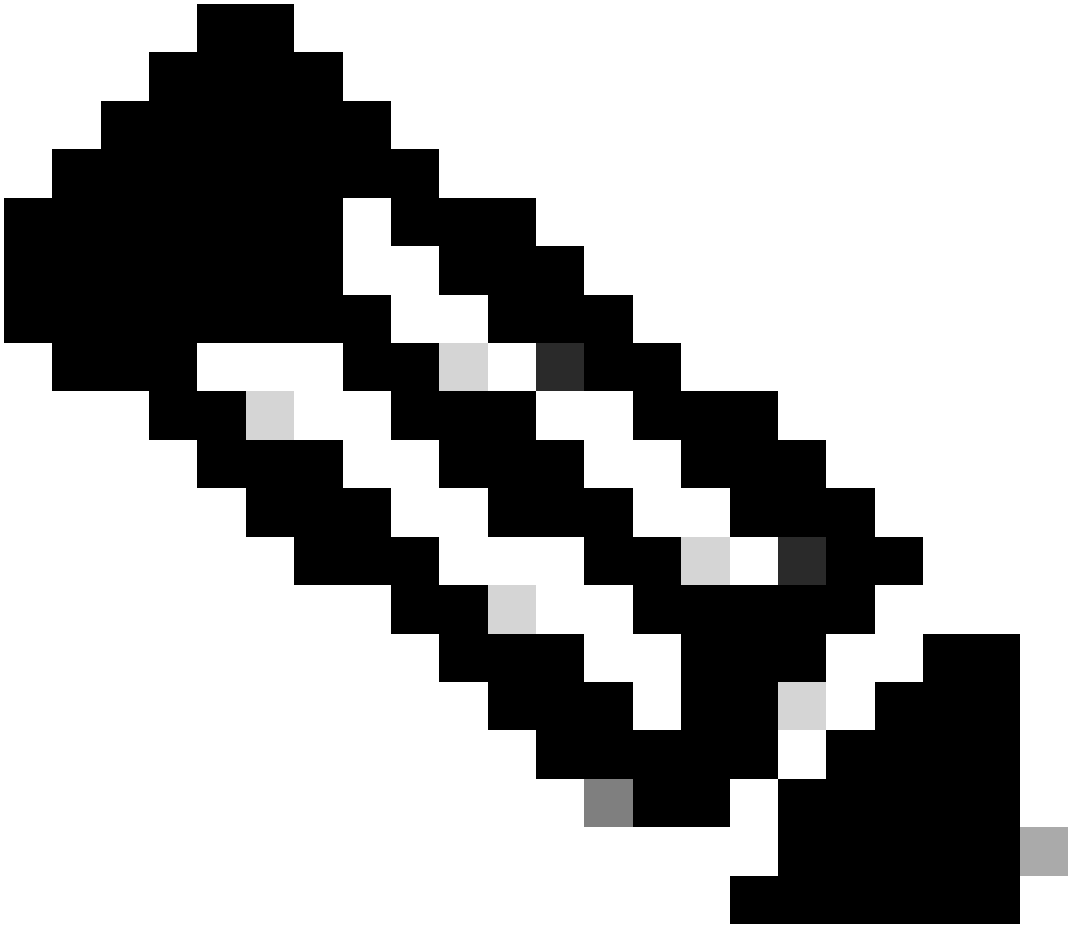
In diesem Dokument wird die Umbrella Enforcement API für benutzerdefinierte Integrationen beschrieben.

Was ist die Umbrella Enforcement API?

Die Umbrella Enforcement API ermöglicht es Partnern und Kunden mit ihren eigenen SIEM/Threat Intelligence Platform (TIPP)-Umgebungen, Ereignisse und/oder Bedrohungsinformationen in ihre Umbrella-Umgebung einzuschleusen. Diese Ereignisse werden sofort in Transparenz und Durchsetzung umgewandelt, die über den Perimeter und damit die Reichweite der Systeme, die diese Ereignisse oder Informationen zu Sicherheitsbedrohungen generiert haben könnten, hinausgehen können.

Die Durchsetzungs-API kann Ereignisse in dem in dieser API-Dokumentation beschriebenen

generischen Ereignisformat aufnehmen und kann ADD-, DELETE- oder LIST-Funktionen unterstützen.



> Anmerkung: Wenn Sie nicht über die Umbrella Enforcement API für benutzerdefinierte Integrationen in Ihr Umbrella Dashboard verfügen und Zugriff benötigen, [wenden Sie sich bitte an Ihren Cisco Umbrella-Vertreter.]

Warum sollte ich es verwenden?

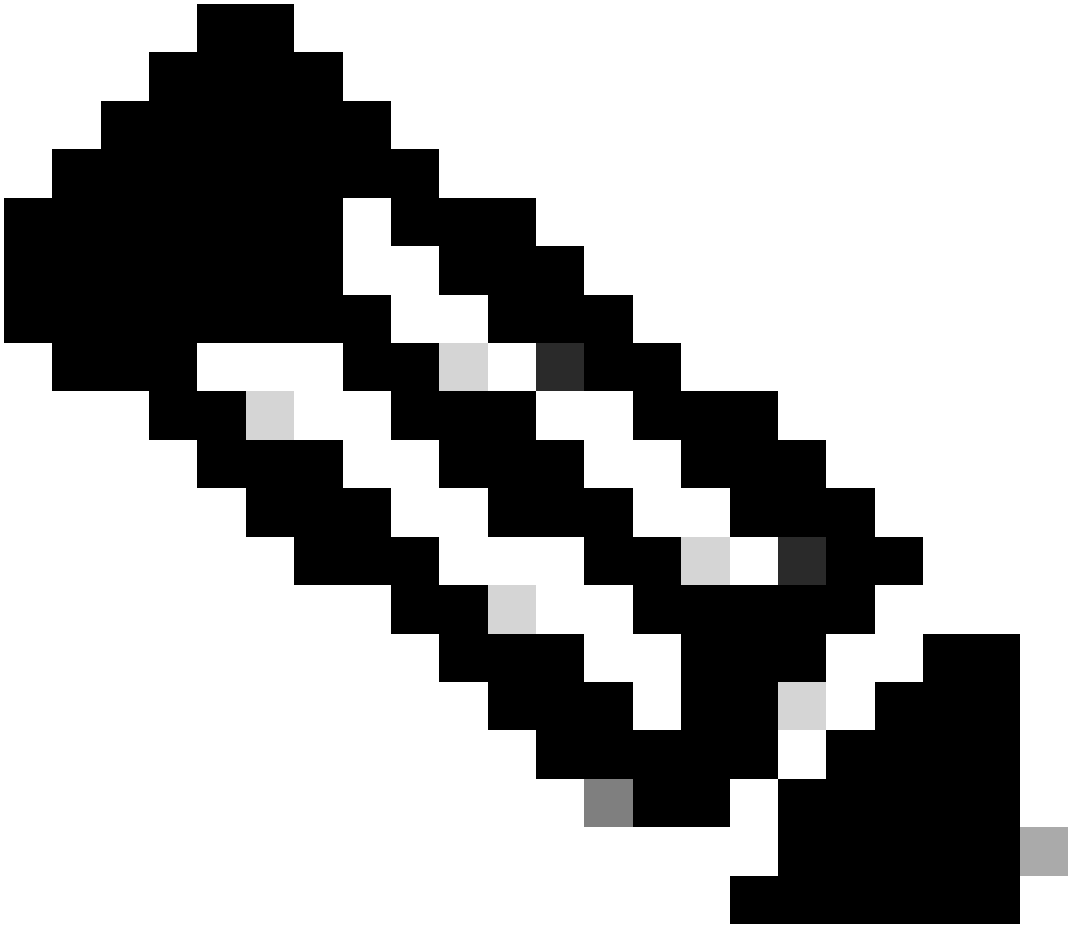
Möglicherweise verarbeiten, verwalten und verwalten Sie bereits Ihr eigenes Threat-Intelligence-System und Ihre eigenen Threat-Intelligence-Prozesse, die den Wunsch nach Aktionen auf als schädlich oder verdächtig erkannten Domänen nach sich ziehen. In diesem Fall können Sie die Durchsetzungs-API verwenden, um diesen Prozess zu automatisieren und den Schutz sofort anhand der Domänen durchzusetzen, die mit dem Ereignis verknüpft sind, sobald entschieden wurde, dass ein Ereignis behandelt werden muss (z. B. durch Umwandlung in Schutz), anstatt manuell Schutz zu Umbrella hinzuzufügen.

So kann sich Ihr Sicherheitsteam auf die Nachforschungen konzentrieren, anstatt Umbrella fortlaufend zu konfigurieren. So kann Ihr Sicherheitsteam innerhalb der Tools und Prozesse bleiben, ohne zum Umbrella Dashboard springen zu müssen, um Ziellisten zu aktualisieren. Im Wesentlichen können Sie eine Zielliste in Umbrella aus einer externen Quelle erstellen, die Sie direkt über die API verwalten. Anschließend können Sie diese Ziele für Identitäten in Umbrella blockieren.

Wie würde ich es verwenden?

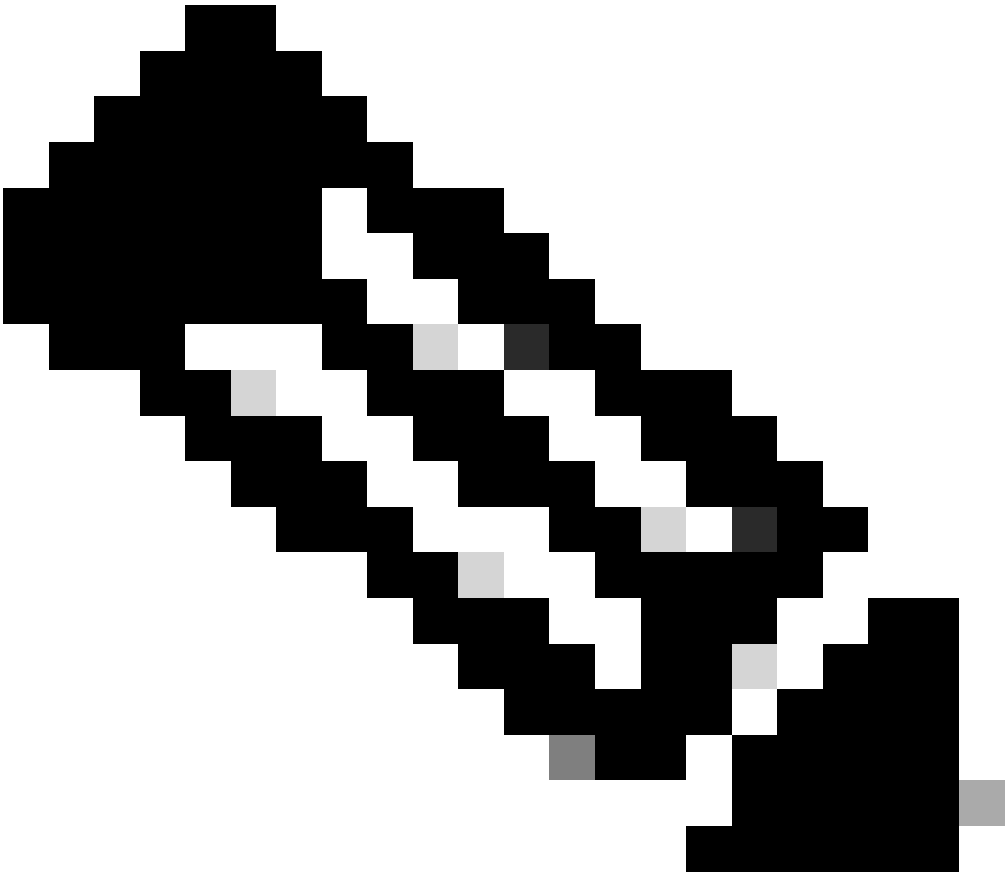
Hinzufügen eines Ereignisses zur Durchsetzungs-API

Sobald ein Ereignis hinzugefügt wurde, versucht die Durchsetzung, Domänen aus dem Ereignis zu extrahieren.



> Anmerkung: Unterstützung für IP-Adressen und URLs wird zu einem späteren Zeitpunkt hinzugefügt.

- Ein Ereignis kann beliebig viele der ursprünglichen Ereignisdetails enthalten, muss jedoch die in der API-Dokumentation beschriebenen Spezifikationen erfüllen.



Anmerkung: Eventuelle spätere Unterstützung für das Aufdecken von Ereignisdetails im Umbrella Dashboard.

- Wenn eine Domäne extrahiert wird, wird sie durch das Cisco Umbrella Security Graph validiert, um sicherzustellen, dass es sich nicht um eine zweifelsfrei funktionierende Domäne handelt, die wahrscheinlich zu Fehlalarmen führt oder anderweitig durch das Cisco Umbrella Security Graph als schädlich eingestuft wird.
- Wenn die Validierung bestanden wird (z. B. weil die Blockierung unbekannt und sicher ist), wird sie einer Zielliste hinzugefügt, die mit dieser benutzerdefinierten Integration verknüpft ist, und im Umbrella Dashboard als benutzerdefinierte Sicherheitskategorie angezeigt.
- Die benutzerdefinierte Sicherheitskategorie kann je nach Richtlinie blockiert oder zugelassen werden, um sowohl die aktive Durchsetzung als auch die passive "Überprüfung" verdächtiger Anforderungen zu ermöglichen.

LIST-Domänen für eine Durchsetzungs-API-Liste

- Wenn der Workflow das Aufheben der Blockierung von Domänen umfasst, die aufgrund zuvor eingefügter Ereignisse blockiert wurden, stellt eine LIST-Anforderung alle Domänen bereit, die derzeit in der Zielliste enthalten sind, die dieser Integration zugeordnet ist.

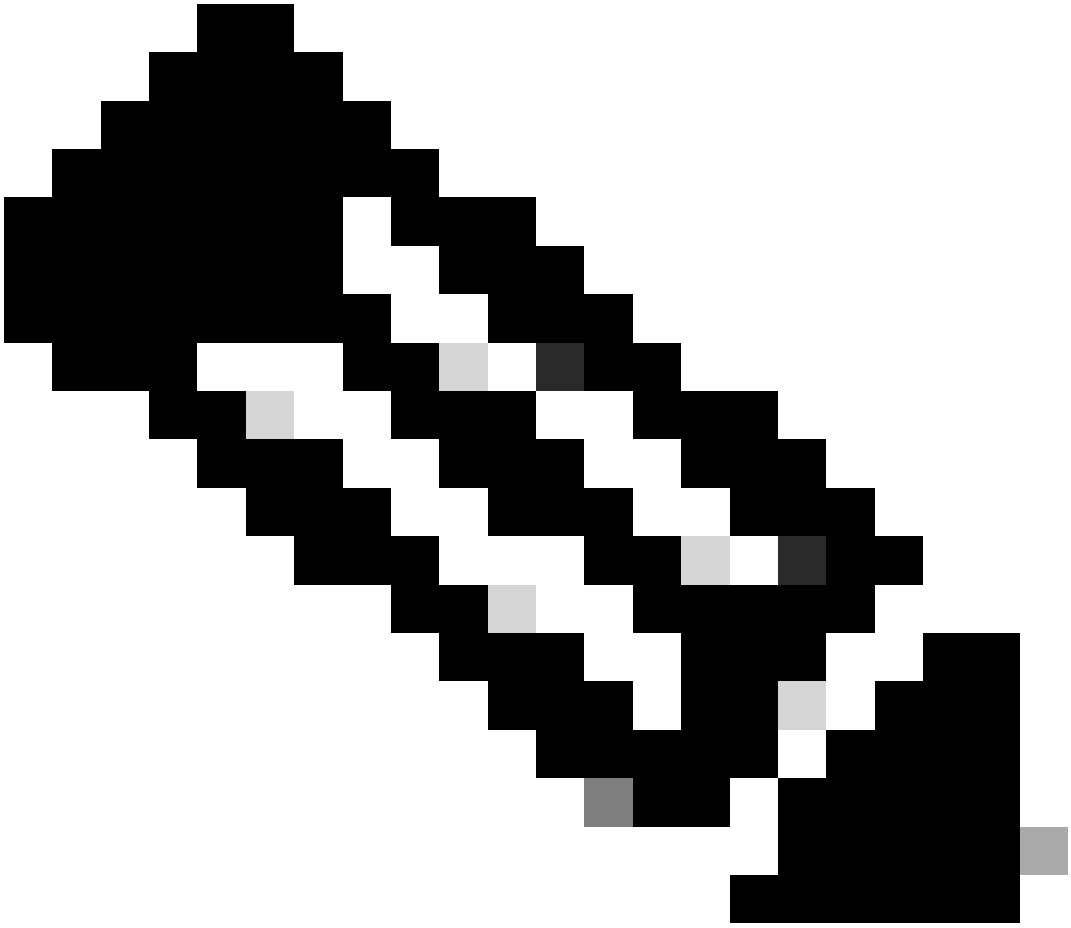
Domäne aus Durchsetzungs-API-Liste LÖSCHEN

- Wenn der Workflow das Aufheben der Blockierung von Domänen umfasst, die aufgrund zuvor eingefügter Ereignisse blockiert wurden, können Sie mit einer DELETE-Anforderung eine Domäne aus der Zielliste entfernen, die dieser Integration zugeordnet ist.
- Wenn eine eingehende DNS-Anforderung von einer Ihrer Umbrella-Identitäten für eine Domäne in der benutzerdefinierten Integrationszielliste bestimmt ist, wird sie abhängig von der Sicherheitseinstellung der benutzerdefinierten Integration blockiert oder zugelassen, die mit der Richtlinie verknüpft ist, die sie ausgelöst hat.
- Die Ergebnisse werden zusammen mit allen anderen Umbrella-Ereignissen protokolliert, auf die über die Aktivitätssuche oder über Amazon S3 über die S3-Integration zugegriffen werden kann. Aus diesem Grund kann der mit der benutzerdefinierten Integration verbundene Datenverkehr optional wieder in Ihr SIEM/TIPP aufgenommen und die Feedback-Schleife geschlossen werden.

Exemplarische Vorgehensweise für die Verwendung der Durchsetzungs-API

Schritt 1: Individuelle Integration

Sie können bis zu 10 kundenspezifische Integrationen gleichzeitig vornehmen.



Anmerkung: Wenn es sich bei der Organisation um eine untergeordnete Organisation eines Umbrella MSP, MSSP oder MOC handelt, werden benutzerdefinierte Integrationen, die von der Konsolenebene freigegeben werden, angezeigt, bevor auf der untergeordneten Organisationsebene Integrationen erstellt werden.

1. Navigieren Sie in Umbrella zu Richtlinien > Richtlinienkomponenten > Integrationen, und klicken Sie auf Hinzufügen.
2. Fügen Sie einen Namen für die benutzerdefinierte Integration hinzu, und klicken Sie auf Erstellen.
3. Erweitern Sie Ihre neue benutzerdefinierte Integration, aktivieren Sie Aktivieren, kopieren Sie die Integrations-URL, und klicken Sie dann auf Speichern.

Phase 2: Erstellen Sie Ihr(e) benutzerdefiniertes(n) Skript(e).

1. Siehe die Beispielskripte generate_event und delete_domain im Anhang dieses Dokuments oder verwenden Sie die API-Dokumentation, um eigene Skripte zu erstellen, um die richtig

formatierten Anforderungen für das Generieren von Ereignissen oder das Löschen oder Auflisten von Domänen zu generieren. Sie sollten in diesen Skripts in Zukunft die benutzerdefinierte Integrations-URL verwenden.

Schritt 3: Ein Beispielereignis einbringen

1. Verwenden Sie das von Ihnen erstellte Skript, um ein Ereignis in die benutzerdefinierte Integration einzufügen. In unserem Beispiel haben wir ein Ereignis mit der Domäne "creditcards.com" eingefügt.

Schritt 4: Zielliste im Umbrella Dashboard überprüfen

1. Zurück zu Einstellungen > Integrationen und in der Tabelle erweitern Sie Ihre benutzerdefinierte Integration.
2. Klicken Sie auf Domains anzeigen. Eine durchsuchbare Liste der hinzugefügten Domänen wird angezeigt, und Ihr Beispielereignis aus Schritt 4 befindet sich jetzt in der Liste.

Schritt 5: Überprüfen Sie das Admin-Audit-Protokoll.

1. Eine weitere Möglichkeit zum Überprüfen der Aktivitäten im Zusammenhang mit der benutzerdefinierten Integration besteht darin, das Admin-Audit-Protokoll zu überprüfen.
2. Navigieren Sie zu Reporting > Admin Audit Log.
3. Geben Sie unter Filters (Filter) den Namen der benutzerdefinierten Integration in Filter by Identities & Settings (Nach Identitäten und Einstellungen filtern) ein, und klicken Sie dann auf Run Filter (Filter ausführen).

Wenn Sie den Eintrag erweitern, sehen Sie jetzt das Ereignis, das dazu geführt hat, dass das Beispielereignis (creditcards.com) zu Ihrer benutzerdefinierten Integration hinzugefügt wurde.

Optionaler Schritt: Auflisten oder Löschen von Domänen

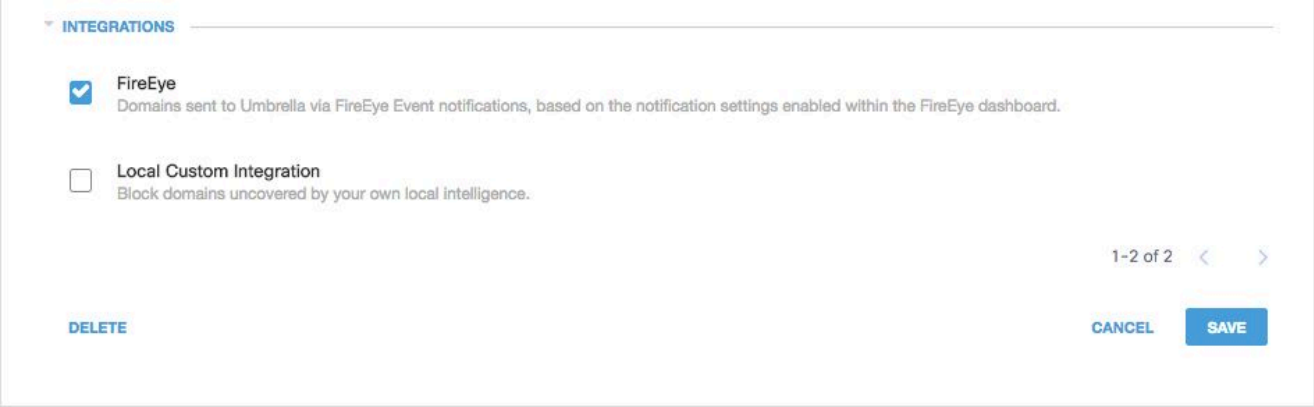
Möglicherweise möchten Sie auch testen, um sicherzustellen, dass Sie Domänen bei der benutzerdefinierten Integration auflisten und Domänen löschen können, falls Sie diese nicht mehr für die Domäne durchsetzen oder in Ihrer Integration beibehalten möchten. Führen Sie die in der API-Dokumentation beschriebenen Schritte aus, um Domänen aufzulisten und zu löschen.

Sicherheitseinstellungen konfigurieren

Nachdem Sie überprüft haben, dass Sie Ereignisse einschleusen (und optional Domänen auflisten und löschen) können, können Sie konfigurieren, was mit DNS-Anforderungen von Ihren Identitäten geschehen soll, die für Domänen in der Sicherheitskategorie der benutzerdefinierten Integration bestimmt sind.

1. Navigieren Sie zu Richtlinien > Sicherheitseinstellungen, und überprüfen Sie unter

Integrationen die aktivierte Integration (in diesem Beispiel FireEye), und klicken Sie auf Speichern.

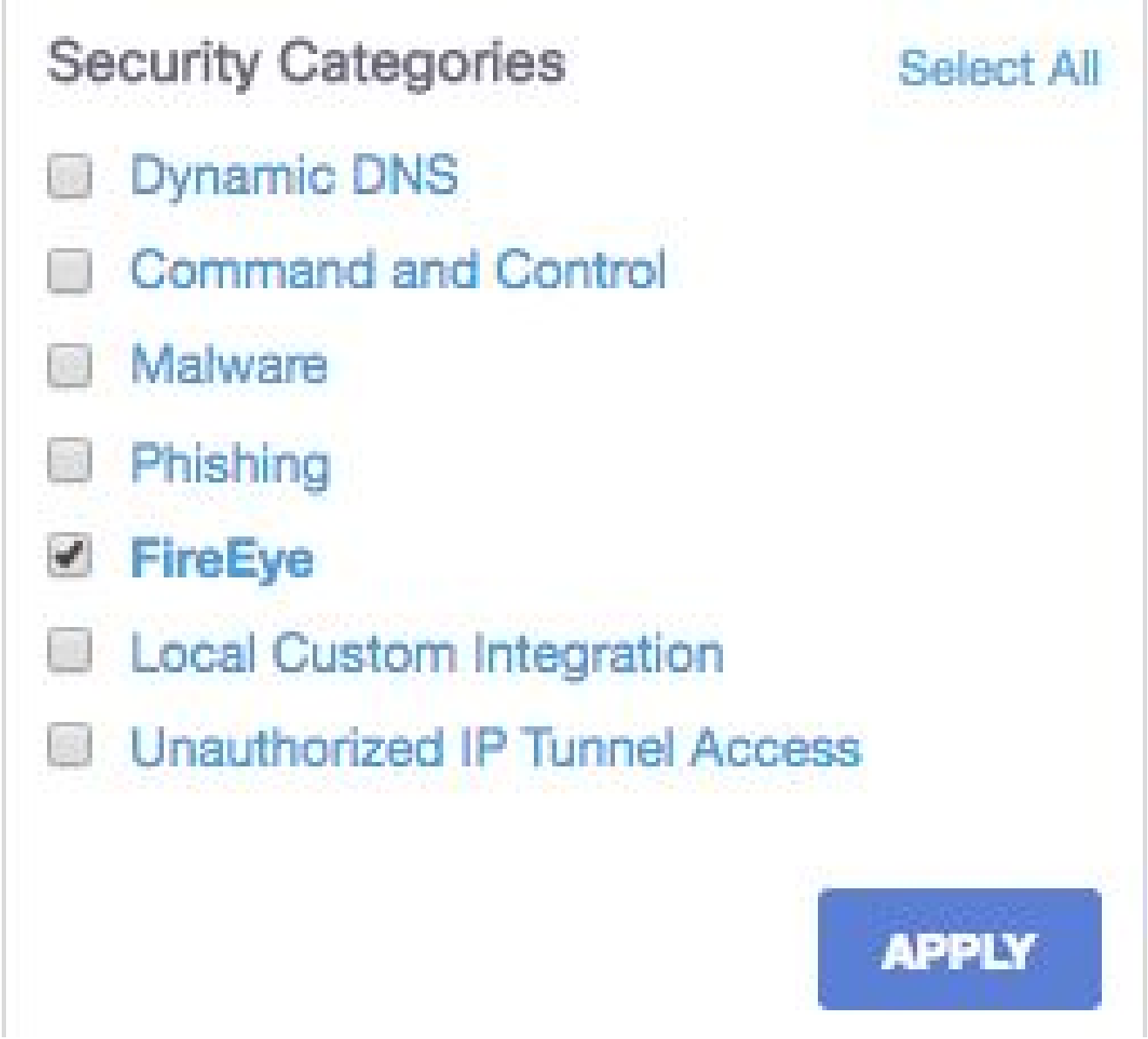


115014145103

Reporting für Ihre benutzerdefinierte Integration anzeigen

Generieren Sie DNS-Anfragen von einer Ihrer Identitäten (z. B. Netzwerke oder Roaming-Computer), die für die Domäne in Ihrer benutzerdefinierten Integration bestimmt sind ("creditcards.com" in unserem Beispiel). Aus Sicht des Clients wird jetzt je nach Konfiguration der Sicherheitseinstellungen der entsprechende Block oder das Ergebnis für die Genehmigung angezeigt.

1. Navigieren Sie zu Reporting > Activity Search, und wählen Sie unter Security Categories Ihre benutzerdefinierte Integration (in diesem Beispiel FireEye) aus, um den Bericht so zu filtern, dass nur die Sicherheitskategorie für FireEye angezeigt wird.

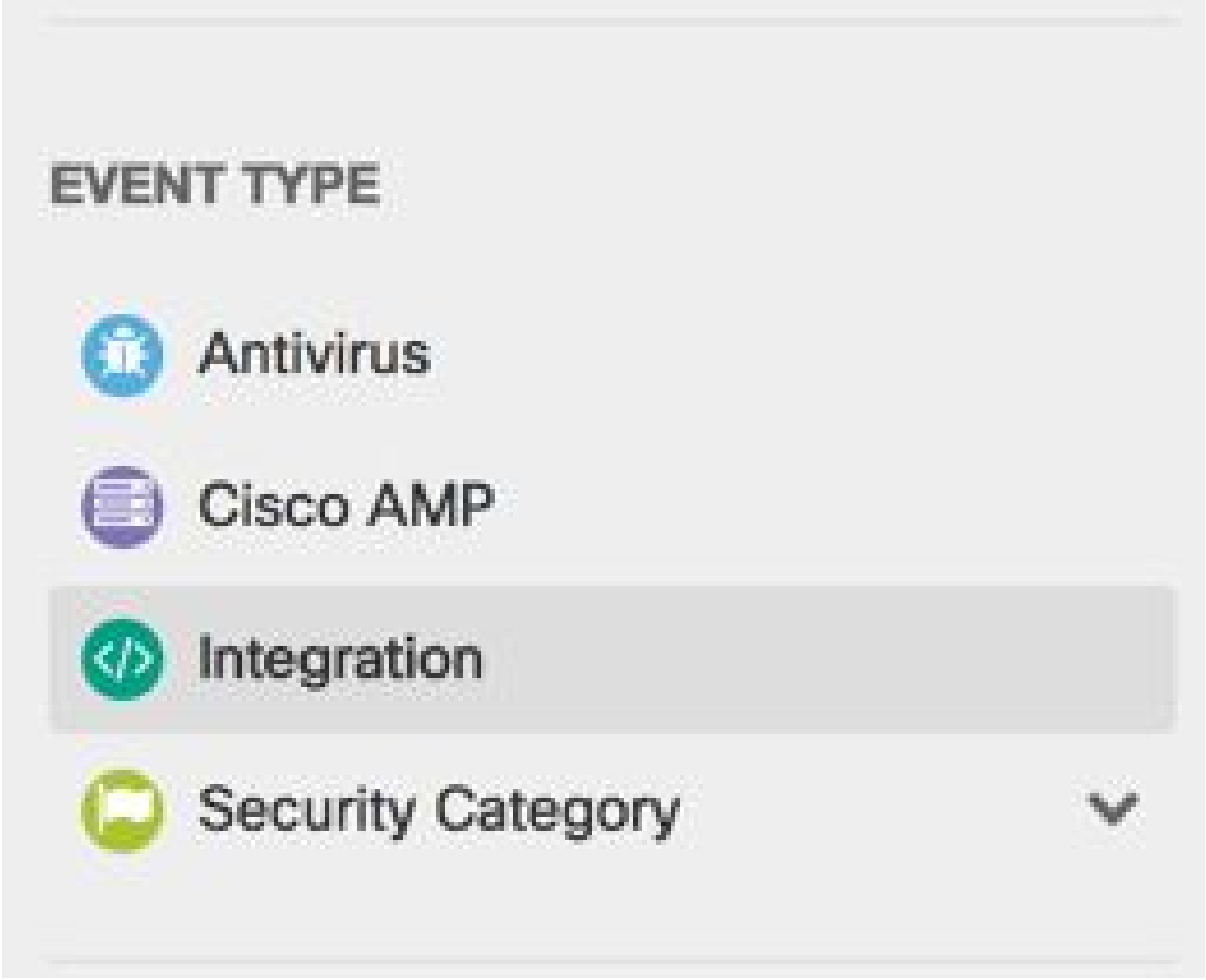


115013981706

2. Klicken Sie auf Apply (Anwenden), um die Aktivität für den im Bericht ausgewählten Zeitraum anzuzeigen.

Sie können auch den Bericht "Activity Volume" (Aktivitätsvolumen) anzeigen, um die Snapshot- oder Trendberechnungsberichte einschließlich Ihrer benutzerdefinierten Integration(en) anzuzeigen.

1. Navigieren Sie zu Reporting > Security Activity Volume.
2. Wählen Sie unter Ereignistyp die Option Integration aus.



115013982286

Konfigurieren Sie Ihre S3-Integration für Protokollspeicher und -verbrauch (optional)

Wenn Sie dann Ihre Umbrella-Protokolle mit allen Anforderungen für Ihre Umgebung an Ihre SIEM/TIPP-Umgebung zurücksenden möchten, können Sie dies mit unserer S3-Integration tun, mit der Sie Ihre DNS-Aktivitätsereignisse zurückstreamen können.

Anhang: Beispielskripte

Diese Perl-Skripte bieten Anleitungen dazu, wie Sie ein Ereignis für Ihre benutzerdefinierte Integration generieren können. Ersetzen Sie in beiden Skripten den customerKey-Wert aus Ihrer Integration. Hinweis: Diese Skripts werden als Beispiele bereitgestellt. Unter Umständen müssen sie angepasst oder aktualisiert werden.

generate_event.pl:

```
#!/usr/bin/perl -w

# Custom integration - ADD EVENT URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/events?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $json_blob = "{
    \"alertTime\" : \"2013-02-08T11:14:26.0Z\",
    \"deviceId\" : \"ba6a59f4-e692-4724-ba36-c28132c761de\",
    \"deviceVersion\" : \"13.7a\",
    \"dstDomain\" : \"$domain\",
    \"dstUrl\" : \"http://$domain/a-bad-url\",
    \"eventTime\" : \"2013-02-08T09:30:26.0Z\",
    \"protocolVersion\" : \"1.0a\",
    \"providerName\" : \"Security Platform\"
}";

my $curl_request = "curl '" . $cust_key . "' -v -X POST -H 'Content-Type: application/json' -d '" . $js

my $results = exec($curl_request);
```

delete_domain.pl:

```
#!/usr/bin/perl -w

# Custom integration - DELETE URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/domains?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $curl_request = "curl '" . $cust_key . "&where[name]=" . $domain . "' -v -i -g -X DELETE -H 'Content
my $results = exec($curl_request);
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.